

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF:

- | | |
|---|----------------|
| 1) Black iPhone, crack on front left corner and several cracks on back (FCPD Item # 9) | No. 1:25-sw-17 |
| 2) Black Samsung, with case, QR sticker on back, glossy finish back (FCPD Item #10) | No. 1:25-sw-18 |
| 3) White iPhone S, Model A1633, FCC ID: BCG-E2946A, IC: 579C-E2946A (FCPD Item #11) | No. 1:25-sw-19 |
| 4) Black iPhone, purplish face, Apple logo on back (FCPD Item #12) | No. 1:25-sw-20 |
| 5) Black iPhone, Model A1778, FCC ID: BCG-E3091A, with retail sticker/barcode on back (FCPD Item #13A) | No. 1:25-sw-21 |
| 6) Gray Motorola, with Motorola symbol on back, 50MP/Quad Pixel (FCPD Item #13B) | No. 1:25-sw-22 |
| 7) Black Samsung, IMEI 350239335722617, QR sticker on back (FCPD Item #13C) | No. 1:25-sw-23 |
| 8) Gray Motorola Razr (FCPD Item #13D) | No. 1:25-sw-24 |
| 9) Black Samsung, IMEI 359147523653240 (FCPD Item #13E) | No. 1:25-sw-25 |
| 10) Gray Motorola, with Motorola symbol on back, 50MP/Quad Pixel (FCPD Item #13F) | No. 1:25-sw-26 |
| 11) Blue Samsung, IMEI 352271522724674, QR sticker on back (FCPD Item #13G) | No. 1:25-sw-27 |
| 12) Silver iPhone, Model A1522, FCC ID: BCG-E2817A, IC: 579C-E2817A, IMEI: 354451060223564 (FCPD Item #13H) | No. 1:25-sw-28 |
| 13) Purple iPhone, QR sticker on back with numbers 30202408131 40940369906 (FCPD Item #13I) | No. 1:25-sw-29 |
| 14) Blue iPhone, with clear Pure Gear case, Apple sticker on back (FCPD Item #14) | No. 1:25-sw-30 |

CURRENTLY LOCATED AT 9325
DISCOVERY BOULEVARD, MANASSAS,
VA 20109.

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Charles Rooney, a Special Agent with the Federal Bureau of Investigation (“FBI”),
being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—fourteen cellular telephones in law enforcement possession—which are further described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

2. As a Special Agent with the FBI, I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C) and an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7).

3. I have been a Special Agent since 2008. I am currently assigned to the Violent Crimes Task Force of the Washington, D.C., Field Office. In my capacity as a law enforcement officer, I have conducted arrests and obtained search warrants and court orders. I have investigated violent crimes, including bank robberies, armored car robberies, assaults, carjackings, kidnappings, and threats that have resulted in arrests and convictions.

4. This investigation relates to three individuals: VINCENT HENRY KIRKLAND, JR., JAVON RUSTIN LOUIS PAIGE, and BRIANNA MAMIE OCEOLIA ARCHIE. These three individuals were originally arrested by local law enforcement in August of 2024, on charges stemming from a robbery that occurred at a Boost Mobile store in Alexandria, Virginia on July 25, 2024, and another robbery at a Geeks Zone store in Woodbridge, Virginia on August

13, 2024. On December 10, 2024, criminal complaints were issued in the Eastern District of Virginia charging KIRKLAND and PAIGE with violating 18 U.S.C. § 924(c)(1)(A)(ii) (use of a firearm during and in relation to a crime of violence), and ARCHIE with violating 18 U.S.C. § 1951(a) (obstruction of interstate commerce by means of robbery), all in relation to the robbery that occurred at the Geeks Zone in August 2024. Your Affiant swore out the affidavit in support of the three criminal complaints. KIRKLAND, PAIGE, and ARCHIE have since been arrested by the FBI and have had their initial and preliminary/detention hearings within the Eastern District of Virginia. Criminal histories for KIRKLAND, PAIGE, and ARCHIE revealed that all three had previous felony convictions.

5. Based on the facts set forth in this Affidavit, there is probable cause to search the devices, which were seized in connection with this investigation, for evidence, fruits, instrumentalities, and/or contraband of 18 U.S.C. § 924(c)(1)(A)(ii) (use of a firearm during and in relation to a crime of violence), 18 U.S.C. § 1951 (obstruction of interstate commerce by means of robbery), 18 U.S.C. § 922(g) (possession of a firearm by a prohibited person), and 18 U.S.C. § 371 (conspiracy), as they relate to the robberies of the Boost Mobile store located at 6531 Little River Turnpike, Alexandria, Virginia and the Geeks Zone store located at 15060 Cardinal Drive, Woodbridge, Virginia, which took place in July and August of 2024, respectively (the “TARGET OFFENSES”), as described in Attachment B.

6. The facts and information contained in this Affidavit are based upon my training and experience, participation in investigations, personal knowledge, and observations during the course of this investigation, as well as the observations, training, and experience of other agents and law enforcement officers involved in this investigation. All observations not personally

made by me were relayed to me by the individuals who made them or are based on my review of records, documents, and other physical evidence obtained during this investigation.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

8. The property to be searched includes fourteen cellular telephones, currently in the custody of the FBI's Northern Virginia Resident Agency, 9325 Discovery Boulevard, Manassas, VA 20109, within the Eastern District of Virginia. These devices are associated with KIRKLAND and will be referred to in this Affidavit as the "**KIRKLAND DEVICES.**" The **KIRKLAND DEVICES** were originally seized by the Fairfax County Police Department ("FCPD") on August 29, 2024, pursuant to a search warrant that was executed at KIRKLAND'S residence located at 6603 Lawndale Drive, Apt. T1, Falls Church, VA 22042. The **KIRKLAND DEVICES** were provided to your Affiant on January 8, 2025 by Detective Adam Mancini of the FCPD.

9. The applied-for warrant would authorize the forensic examination of the **KIRKLAND DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE AS TO THE OFFENSES¹

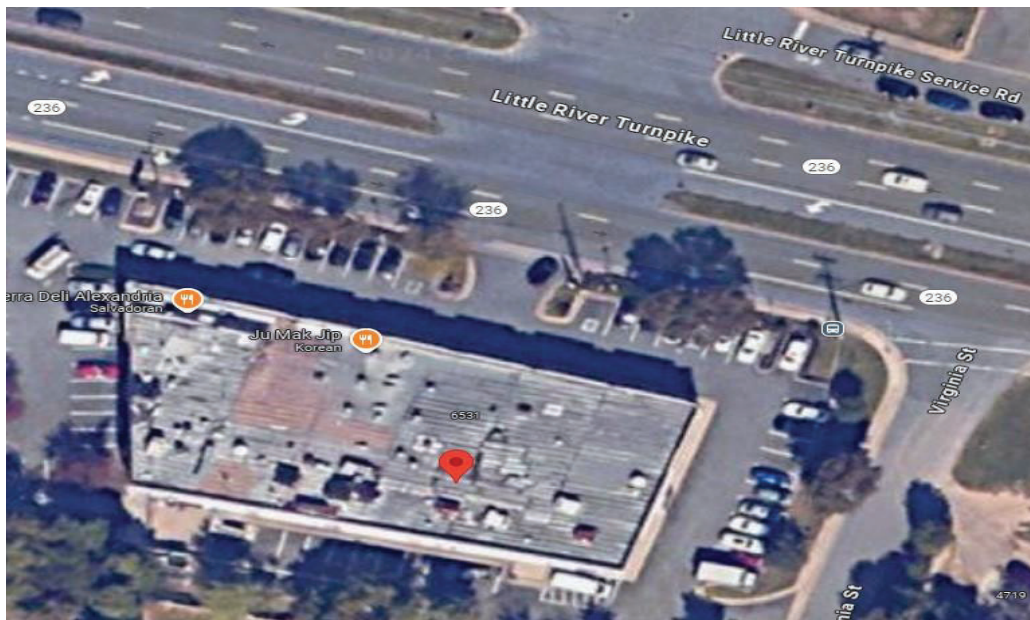
10. The FBI, the FCPD, and Prince William County Police Department ("PWCPD") have been investigating a series of cellular phone store robberies that occurred in the summer of

¹ This section in support of probable cause as to the offenses is substantially the same as the probable cause section in the affidavit in support of the aforementioned criminal complaints. See Case No. 1:24-mj-487, ECF Nos. 1-3 (Complaints) & 4 (Affidavit).

2024. As detailed below, law enforcement believes that PAIGE and KIRKLAND participated in a robbery of a Boost Mobile store on July 25, 2024, during which PAIGE brandished a firearm, and that PAIGE, KIRKLAND, and ARCHIE participated in a robbery of a Geeks Zone store on August 13, 2024, during which both PAIGE and KIRKLAND brandished firearms.

The Boost Mobile Robbery

11. On July 25, 2024, at approximately 11:19 a.m., two subjects robbed a Boost Mobile store (“Boost Mobile”) located at 6531 Little River Turnpike, Alexandria, Virginia, which is in Fairfax County within the Eastern District of Virginia. Boost Mobile, which is located in a shopping center with other stores attached on both sides, is a commercial establishment that sells cellular phones and other products and is a business that was engaged in and that affected interstate commerce. In addition to taking items from three victims inside the store, the subjects stole merchandise from Boost Mobile, including approximately 41 phones and approximately \$5,000 in United States currency.



(Google Maps Aerial View of 6531 Little River Turnpike, Alexandria, Virginia)

12. Based on surveillance video from Boost Mobile, which included an audio recording from a camera inside the store, the two subjects can be described as follows. The first individual – referred to herein as “Subject 1” (who, as explained in this affidavit, was later identified as KIRKLAND) – wore dark clothing, gray New Balance sneakers, white gloves with red/orange palms, a hood pulled up over his head, and his face partially covered by what appeared to be a black mask but with his eyes and nose visible. Subject 1 carried a dark colored backpack. The second individual – referred to herein as “Subject 2” (who, as explained in this affidavit, was later identified as PAIGE) – wore a gray top, dark pants, white sneakers with black trim, white gloves with red/orange palms (which appeared similar to those worn by Subject 1), a hood pulled up over his head, and a white covid-style mask that partially covered his face. Subject 2 carried a dark colored backpack and was armed with a black handgun. Both subjects appeared to be black males.



(Subjects 1 & 2 inside Boost Mobile)



(Subject 2 inside Boost Mobile)



(Subject 2's sneakers)

13. According to Boost Mobile video, as both subjects entered the Boost Mobile, they encountered an employee of the store (“Victim 1”), who was assisting a customer (“Victim 2”) at the cash register. Subject 2 pointed his handgun at the two victims. According to the audio recording, one of the subjects initially ordered the two victims to lay on the ground, and ultimately both victims were told to get in the back of the store. Subject 1 started to drag Victim 2 across the floor towards the back and threatened to shoot, before Victim 2 was able to get up and walk to the rear. In the back of the store, the subjects encountered the store manager (“Victim 3”). According to the audio recording, one of the subjects demanded cellular phones, specifically iPhone 15 Pros.

14. Surveillance video captured the movement and actions of both subjects and the victims at the back of the store. Both subjects stomped their feet on the back of Victim 1’s head as he laid on the ground. Subject 2 appeared to stomp his foot down in the area where Victim 2 was lying, but that view was partially obscured. Subject 2 also struck Victim 3 in the back of the head with what appeared to be the butt end of his handgun.

15. According to Boost Mobile video, Subject 1 loaded items from the Boost Mobile into his backpack and a trashcan that was inside the store, and Subject 2 also loaded items from the store into his backpack. Subject 1 fled the store on foot with the trashcan and turned right as he exited, running east. Before departing, Subject 2 leaned over both Victim 1 and Victim 2. It was later determined through interviews that both victims were sprayed in the face with what was believed to have been pepper spray. Based on surveillance video, neither victim appeared to provoke Subject 2 into being pepper sprayed. Subject 2 fled the store, and surveillance video captured him entering the front passenger side door of a silver vehicle, which drove away.

16. Victim 3 called law enforcement, and FCPD responded to the scene and interviewed all three victims. Victim 1 reported that his phone was stolen, and Victim 2 and Victim 3 reported that their wallets were stolen. According to surveillance video, Subject 2 appeared to take personal items from Victim 1 and Victim 2 and, at one point, started hitting an object consistent with a phone against a desk in the back room. Victim 1 was treated by medics at the scene and, based on body worn camera footage, had visible abrasions to his cheek and chin.

17. In addition to video from Boost Mobile, law enforcement recovered surveillance video from other stores within the shopping center, including MetroPCS and Eternal Bridal. Boost Mobile is located between MetroPCS and Eternal Bridal. According to MetroPCS video, at approximately 11:12 a.m., a silver vehicle entered the parking lot of the shopping center from Little River Turnpike and drove east. This vehicle was also seen on the Eternal Bridal video entering the shopping center and driving east in the parking lot. The vehicle continued past Eternal Bridal towards the east end of the shopping center and out of the camera's view. Approximately a minute and a half later, a silver vehicle that appeared to be the same vehicle drove past both Eternal Bridal and MetroPCS. It then slowly reversed and again passed the stores, including Boost Mobile, before driving toward the east end of the shopping center and out of the camera's view.

18. According to Boost Mobile video, at approximately 11:19 a.m., Subject 1 and Subject 2 entered Boost Mobile. Both subjects came from the direction the silver vehicle was last seen in the Eternal Bridal video. At approximately 11:24 a.m., Subject 1 fled Boost Mobile after the robbery and headed east in the parking lot in the direction the silver vehicle was last seen. Approximately forty seconds later, Subject 2 fled Boost Mobile, and the silver vehicle pulled in front of Boost Mobile. According to the Eternal Bridal video, the silver vehicle came from the east end of the shopping center. Based on a review of video from the various cameras located in

the shopping center, the silver vehicle seen at different times is believed to be the same based on color, doors, body style, lights, and wheel style.



(Eternal Bridal video of silver vehicle in parking lot prior to Boost Mobile robbery)

19. Law enforcement received information from a witness who described the getaway vehicle as a silver Mitsubishi Galant with the last four digits of the license plate as either 4967 or 4667. Through database checks, specifically FLOCK, which is a license plate reader (“LPR”) platform, law enforcement identified a silver Mitsubishi Galant with Virginia license plate TVF3999 (“Mitsubishi Galant”) that appeared similar in appearance to that of the getaway vehicle based on images seen in FLOCK.

20. Law enforcement contacted the owner of the Mitsubishi Galant on July 26, 2024, and learned that the vehicle was a rental car. The owner advised that he rents multiple vehicles through Turo, a peer-to-peer car sharing marketplace that allows users to rent cars directly from owners. Beginning on or around June 26, 2024 (i.e., approximately one month before the Boost Mobile robbery), the Mitsubishi Galant was rented to a female renter (referred to herein by her initials A.S.V.S.). The owner advised that at approximately 2:24 p.m. on July 25, 2024 (i.e., 3 hours after the Boost Mobile robbery), that A.S.V.S. asked to trade the Mitsubishi Galant in for another vehicle. On July 26, 2024, the Mitsubishi Galant was traded in for a Honda Accord. The

owner advised that he did not have face-to-face contact during the trade-in. On July 26, 2024, law enforcement conducted a consent search of the Mitsubishi Galant and processed it for evidence, including latent prints. According to a report dated August 16, 2024, the latent prints were examined and at least one print was identified to PAIGE and at least one print was identified to A.S.V.S.

21. FLOCK data placed the Mitsubishi Galant near an Exxon gas station (“Exxon”) located at 6261 Little River Turnpike, Alexandria, Virginia (i.e., approximately one mile from the Boost Mobile), at approximately 9:10 a.m. on July 25, 2024 (i.e., approximately two hours before the Boost Mobile robbery). Exxon surveillance video showed the Mitsubishi Galant enter the parking lot. (Timestamps for the Exxon video appear to be approximately 1 hour behind compared to the FLOCK data.) In video from an exterior camera, the license plate is visible as Virginia tag TVF3999. A black male subject exited the vehicle from the driver’s door. The subject went inside the Exxon and purchased two drinks and what appeared to be a packaged set of white gloves with red/orange palms. (Your affiant later went to this Exxon and confirmed that packaged sets of white gloves with red/orange palms are displayed on the same shelf and appear in the same packaging as the item purchased by the subject.) This subject had long dreadlocks and multiple tattoos on both forearms and wore white sneakers with black trim, which appeared similar to the sneakers worn by Subject 2 in the Boost Mobile robbery.



(Subject purchasing gloves inside Exxon)



(Subject's sneakers inside Exxon)

22. The Mitsubishi Galant in the Exxon video appeared similar to the Boost Mobile robbery getaway vehicle based on color, taillight configuration, hubcaps, black grill, and what appeared to be an air freshener hanging from the rearview mirror. In addition, pictures taken of the Mitsubishi Galant during the consent search on July 26, 2024, showed all those same characteristics, including the air freshener. During the consent search, the Mitsubishi Galant had minor damage including scratches on the right front passenger side bumper. In the Eternal Bridal video, those scratches are faintly visible on the bumper.



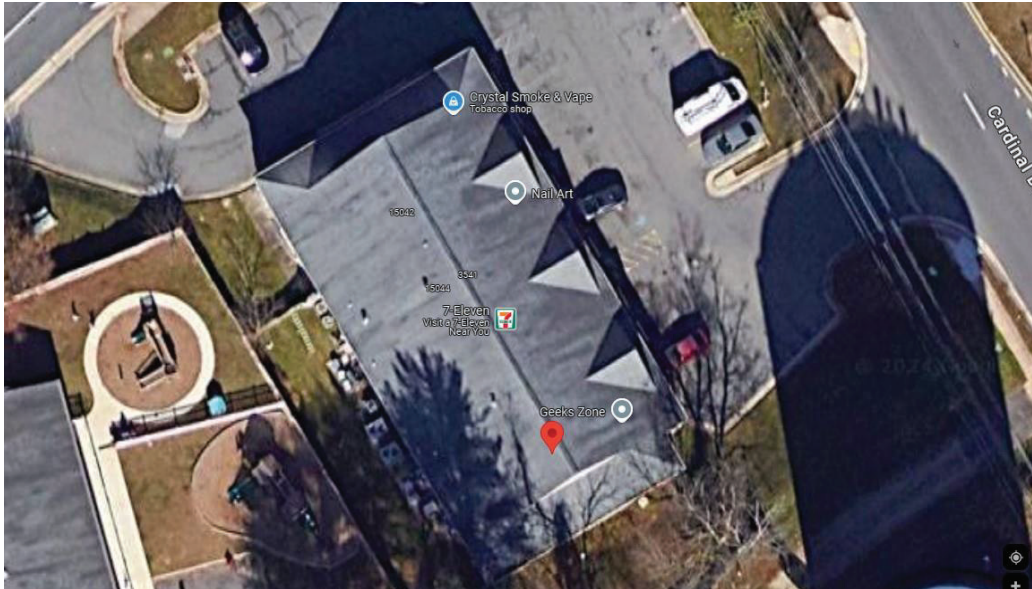
(Mitsubishi Galant at Exxon)



(Mitsubishi Galant at Exxon)

The Geeks Zone Robbery

23. On August 13, 2024, at approximately 12:14 p.m., two subjects robbed the Geeks Zone store (“Geeks Zone”) located at 15060 Cardinal Drive, Woodbridge, Virginia, which is in Prince William County within the Eastern District of Virginia. Geeks Zone is a commercial establishment that sells and repairs merchandise, including cellular phones, tablets, and play stations and is a business that was engaged in and that affected interstate commerce. In addition to taking items from two victims inside the store, the subjects stole merchandise from Geeks Zone, including approximately 46 electronic devices, consisting of cellular phones, tablets, iPads, and PlayStations, and approximately \$2,000 in United States currency.



(Google Maps Aerial View of 15060 Cardinal Drive, Dumfries, Virginia)

24. Based on surveillance video from Geeks Zone, which included an audio recording from a camera inside the store, the two subjects can be described as follows. One individual – referred to herein as “Subject 1” (who, as explained in this affidavit, is believed to be the same as Subject 1 from the Boost Mobile robbery and was later identified as KIRKLAND) – wore a gray hooded sweatshirt, dark pants, New Balance sneakers (which appeared similar to Subject 1’s sneakers in the Boost Mobile robbery), and white gloves with red/orange palms (which appeared similar to the gloves worn by both subjects in the Boost Mobile robbery). Subject 1 had the hood of his sweatshirt pulled up over his head and appeared to be wearing a black mask over the lower portion of his face. Subject 1 was armed with a handgun. The second individual – referred to herein as “Subject 2” (who, as explained in this affidavit, is believed to be the same as Subject 2 from the Boost Mobile robbery and was later identified as PAIGE) – wore a black Reebok sweatshirt with white trim, white shirt underneath, multicolored underwear, dark pants, white sneakers with black trim (which appeared similar to Subject 2’s sneakers in the Boost Mobile robbery), and white gloves with red/orange palms (which appeared similar to the gloves worn by

both subjects in the Boost Mobile robbery). Subject 2 carried a dark duffle bag and was also armed with a black handgun. Subject 2 had the hood of his sweatshirt pulled up over his head and appeared to be wearing a black mask over the lower portion of his face.



(Subject 2's sneakers)

25. At the time of the robbery, Geeks Zone was occupied by an intern of the store ("Victim 1") and the owner of the store ("Victim 2").² According to Geeks Zone video, both subjects entered the store carrying orange traffic cones, which they dropped as they ran toward the back of the store and out of view of the cameras. According to the audio recording, one or both of the subjects ordered the victims to the ground, asking where the money was, and one of the subjects said, "fill it up" and "put the money in the bag" several times. According to the audio recording, one of the subjects counted down from five. The audio recording also captured one subject threatening to shoot, to which the other subject stated: "do not shoot him."

26. According to Geeks Zone video, Subject 1 had Victim 1 go to the front of the store and demanded money from the register. Victim 1 appeared dazed and shook his head. Victim 1

² "Victim 1" and "Victim 2" in the Geeks Zone robbery are different individuals from "Victim 1" and "Victim 2" in the Boost Mobile robbery, though the victims are referred to consistently within the context of each robbery.

was bleeding from the back of his head. Victim 1 was unable to open the register, and Subject 1 pushed Victim 1 back to the rear of the store while saying: "I'm about to shoot you, come back here, you're dead." The Geeks Zone video showed a portion of Subject 1's gun, which appeared to have a tan/brown slide.

27. According to Geeks Zone video, Subject 2 then brought Victim 2 at gun point to the front of the store to open the register. Victim 2 was holding the top of his head, which also appeared to be bleeding. Victim 2 was able to open the register, and Subject 2 then told Victim 2 to go back to the rear of the store. Eventually both subjects brought both victims back to the front of the store. Subject 1 had Victim 1 hold open a dark-colored laundry-type bag as he emptied merchandise from the display cases into it. In addition to the dark-colored laundry-style bag Subject 1 had, Subject 2 had a big duffle bag that he stuffed merchandise into. Subject 1 fled through the front door of the store, followed by Subject 2 several seconds later.

28. Victim 2 called law enforcement, and PWCPD responded to the scene and interviewed the victims. Victim 2 advised that the subjects stole his wallet, which included a few hundred dollars, and that he was struck in the head by one of the subjects with a gun. Victim 1 also advised that he was struck by one of the subjects with a gun and that they took cash from his wallet.

29. Law enforcement canvassed and determined that the subjects originally came from an area to the rear of Geeks Zone. Surveillance video was collected from a tobacco store at the end of the shopping center that showed Subject 1 and Subject 2 walking toward the Geeks Zone prior to the robbery from the direction of the Montclair Montessori School. Both subjects were carrying the orange traffic cones, which they dropped inside Geeks Zone. Both subjects' masks were pulled down at this point, and they both appeared to be black males.



(Subjects 1 & 2 walking toward Geeks Zone)

30. Two witnesses who were together at the time called 911 and reported seeing a vehicle, which they described as a gray Toyota Prius, drop off two black males wearing “hoodies,” one black and the other gray. The witnesses saw the subjects carrying orange traffic cones and walking toward the 7-Eleven, which is in the direction of and in the same shopping center as Geeks Zone. The witnesses saw the subjects return to the same vehicle carrying either large trash bags or duffle bags, and the vehicle ran a red light while fleeing the area. The driver was a heavier set black or Hispanic female, who one of the witnesses described as wearing a light-colored tank top. The witnesses captured pictures of the vehicle. It should be noted that these witnesses were located behind the Geeks Zone and adjacent to the Montclair Montessori School.



(Witnesses' picture of vehicle)

31. On August 20, 2024, law enforcement contacted one of the witnesses, who provided a similar description to the witnesses' 911 call. The witness advised that at the time it happened, the witness believed the vehicle was a Toyota Prius but was now not sure. The witness advised that the vehicle had the look of a Prius. The witness described the driver as a "larger framed," probably a black female who looked young, in her early to mid-twenties. She further described the driver as possibly wearing a peach or off-white sleeveless top. The witness described the driver's hair as curly with volume that was possibly black or brown and might have had bleached tips. When asked, the witness stated that the driver was not wearing glasses. In addition, the witness stated that the female driver was the only one in the vehicle waiting.

Identification of PAIGE, KIRKLAND, and ARCHIE

32. FCPD learned from PWCPD of the Geeks Zone robbery. Through investigative steps already pursued and ongoing by FCPD, investigators knew that A.S.V.S. (the female renter of the Mitsubishi Galant at the time of the Boost Mobile robbery) was renting a Toyota Scion ("Toyota Scion") during the Geeks Zone robbery and was possibly staying at a Red Roof Inn located at 17113 Dumfries Road, Dumfries, Virginia. Through social media analysis, a connection was discovered between A.S.V.S. and a Facebook profile with the name "Javon Page." The Facebook account for "Javon Page" included a series of pictures depicting a black male who matched the subject shown in the Exxon video, including a distinctive tattoo of a woman's face on his forearm. This tattoo could be seen in the Exxon video.

33. At that point, through records including prior police contacts, law enforcement identified the person depicted in the Facebook account for "Javon Page" and the Exxon video as PAIGE.



(Virginia DMV photo of PAIGE)

34. FCPD obtained arrest warrants for PAIGE for the Boost Mobile robbery, and PWCPD arrested him in Manassas, Virginia, on August 14, 2024. At the time of his arrest, law enforcement observed PAIGE near the Toyota Scion and interacting with an individual later identified and whose initials are J.J.M.³ Law enforcement could see what appeared to be a gun located between the driver's seat and middle console of the Toyota Scion.

35. On August 15, 2024, FCPD and PWCPD executed a search warrant at the Red Roof Inn in Dumfries, Virginia, where it was believed PAIGE was staying. During that search, law

³ At the time of PAIGE'S arrest, law enforcement detained and questioned J.J.M. It was reported that J.J.M. had a gap in his front teeth. Video from the tobacco store for the Geeks Zone robbery captured Subject 1 outside the Geeks Zone with his mask pulled down; a review of that video showed that Subject 1 appeared to have a gap in between his front teeth. (At the time of KIRKLAND's later arrest on August 29, 2024, law enforcement who interviewed KIRKLAND advised that KIRKLAND also had a gap between his front teeth.) After questioning, law enforcement determined that J.J.M. was not directly involved in the Geeks Zone robbery, and he was released.

Virginia Department of Corrections records show that J.J.M. was incarcerated at the same correctional institution as PAIGE and KIRKLAND in 2023.

enforcement recovered white sneakers with black trim consistent with Subject 2's sneakers in both robberies.

36. On August 16, 2024, FCPD executed a search warrant for the Toyota Scion and seized a black handgun. In addition, other items seized included: a black Reebok sweatshirt with white trim; several bottles of pepper spray; packaging with Geeks Zone labels and identifications numbers that matched the Geeks Zone inventory list of stolen merchandise; a phone with a Geeks Zone label that was on the Geeks Zone inventory list of stolen merchandise; and a driver's license and birth certificate for Victim 2 from the Boost Mobile robbery. The Reebok sweatshirt was consistent in appearance to what was viewed in the Geeks Zone video.



(Gun from Toyota Scion)

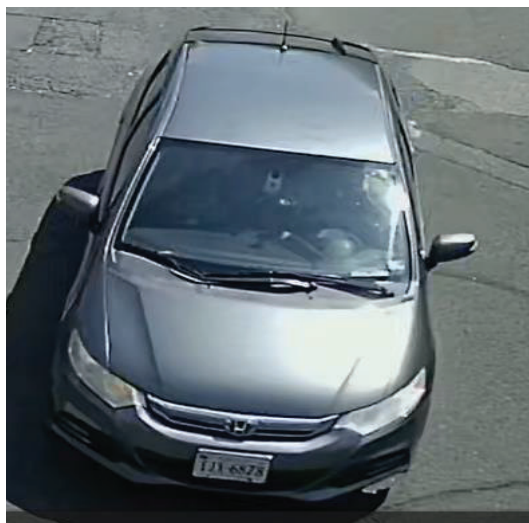


(Gun from Geeks Zone ATI Bulletin)

37. Law enforcement collected surveillance video from the Red Roof Inn and surrounding area that revealed the following: On August 13, 2024, prior to the Geeks Zone robbery, PAIGE was both inside and outside the Red Roof Inn. (According to Google Maps, the Red Roof Inn is approximately 4.5 miles from Geeks Zone.) PAIGE wore white sneakers with black trim (which appeared similar to the sneakers worn by Subject 2 in both the Boost Mobile and Geeks Zone robberies) and multicolored underwear (which appeared similar to the

multicolored underwear worn by Subject 2 in the Geeks Zone robbery). Based on another camera angle, a person believed to be PAIGE retrieved items from the Toyota Scion. A gray vehicle, which was later determined to be a Honda (“Honda”), arrived at the Red Roof Inn. A black male wearing a gray hooded sweatshirt and dark pants (which appeared similar to the clothing worn by Subject 1 in the Geeks Zone robbery) exited the front passenger seat of the Honda, walked over to PAIGE at the Toyota Scion, and later returned to the front passenger seat of the Honda. PAIGE eventually got into the Honda’s rear passenger driver’s side seat and was carrying a bag, and the Honda exited the parking lot of the Red Roof Inn.

38. As the Honda navigated to the main road, it passed surveillance cameras located at an adjacent Motel 6. (There is a discrepancy in video timestamps in that the timestamp of the Red Roof Inn video is approximately 12 minutes behind the timestamp of the Motel 6 video.) Motel 6 video showed that the Honda appeared to have a Virginia license plate. Law enforcement attempted variations of the plate that could be read from the video surveillance and eventually determined the vehicle to be a 2012 Honda bearing Virginia license TJX6878. The vehicle was registered to ARCHIE. The Honda is a hatchback and has features similar to that of a Toyota Prius, which witnesses described as the Geeks Zone robbery getaway vehicle.



(Motel 6 video still images of vehicle)

39. Surveillance video from the Red Roof Inn also showed a similar looking Honda return shortly after the Geeks Zone robbery. Based on the Red Roof Inn video, PAIGE exited the rear driver's side passenger door. Paige wore a white shirt and white sneakers with black trim and appeared to have the black sweatshirt with white trim draped over his shoulder. PAIGE carried a black duffle bag similar to what Subject 2 carried; notably, the shoulder strap of the black duffle bag was not completely attached in both the Red Roof Inn video and the Geeks Zone video.



(Still image of vehicle at Red Roof Inn before robbery)



(Still image of vehicle at Red Roof Inn after robbery)

40. Law enforcement obtained an inventory list of the stolen items from both the Boost Mobile and Geeks Zone robberies, including the IMEI numbers of cellular phones. Through an IMEI search, law enforcement learned that numerous stolen cell phones were sold to EcoATMs

located inside stores. An EcoATM is an automated kiosk that pays cash instantly for recycling cell phones to help reduce electronic waste. According to the EcoATM website, a state-issued identification is required to sell a device.

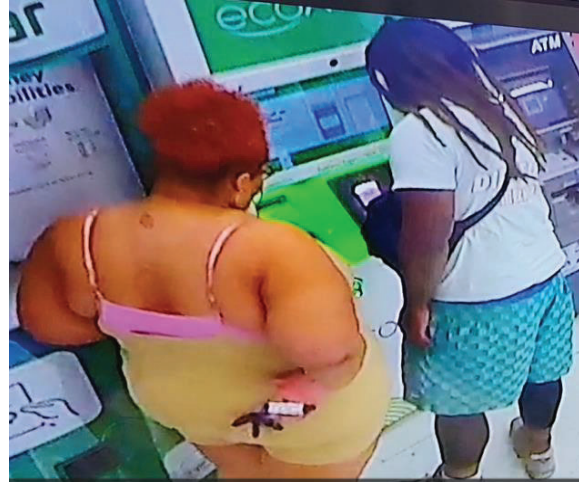
41. On August 13, 2024, at approximately 1:15 p.m. (i.e., approximately one hour after the Geeks Zone robbery), phones taken in the Geeks Zone robbery were sold at an EcoATM located inside a Walmart at 5885 Kingstowne Boulevard, Alexandria, Virginia. According to Google Maps, the Walmart is approximately 20 miles from the Red Roof Inn. EcoATM records showed that a black male using a District of Columbia driver's license bearing a name with initials K.M. sold approximately five phones taken in the Geeks Zone robbery. (The black male using the EcoATM was later determined to be KIRKLAND, who presented an identification with someone else's name; the District of Columbia driver's license bearing the name with initials K.M., which was recovered after the arrest and execution of the search warrant at KIRKLAND's residence, was located inside a wallet also containing an identification in KIRKLAND's name.) The black male had long dreadlocks, wore gray New Balance sneakers (which appeared similar to Subject 1's sneakers in both robberies), and appeared to wear a GPS monitoring device on his ankle.

42. At that time, the black male was accompanied by a female who attempted to sell a phone to the EcoATM that was taken in the Geeks Zone robbery. This female also sold another phone at the time to the EcoATM that was not on the Geeks Zone stolen inventory list. The female matched the witnesses' description of the getaway driver for the Geeks Zone robbery. Surveillance video and still images showed that the female, who wore a tan/cream-colored sleeveless bodysuit, was heavier set with somewhat curly hair that appeared to be dyed on the ends. The female provided a Virginia driver's license with the name BRIANNA MAMIE OCEOLIA ARCHIE (i.e., the registered owner of the Honda believed to be the Geeks Zone robbery getaway vehicle).

Surveillance video and still images of the Walmart parking lot revealed that ARCHIE and the black male arrived in what appeared to be the Honda and walked into the store together. Based on surveillance video, ARCHIE and the black male at times stood together; at one moment, ARCHIE touched the forearm area of the black male and picked something off his shirt; and, at another point, ARCHIE held a phone to her ear, while the black male stood in front of the EcoATM.



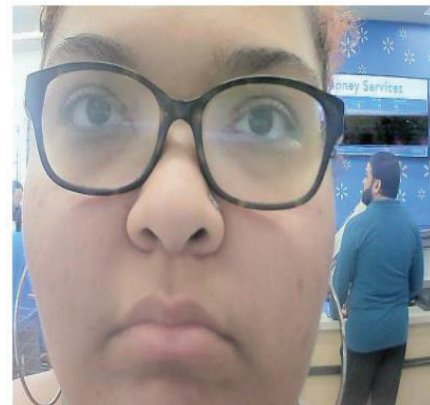
(Inside Walmart)



(Inside Walmart at EcoATM)



(EcoATM image of KIRKLAND using K.M. DC ID)



(EcoATM image of ARCHIE)

43. According to EcoATM records, ARCHIE sold several other phones both before and after the Geeks Zone robbery. At approximately 7:12 p.m. on August 11, 2024 (i.e., approximately 19 days after the Boost Mobile robbery), ARCHIE sold a cellular phone taken in

the Boost Mobile robbery to an EcoATM inside the same Walmart. On August 13, 2024, at approximately 5:13 p.m. (i.e., approximately 5 hours after the Geeks Zone robbery), at the same Walmart, ARCHIE sold two cellular phones, one of which was taken in the Geeks Zone robbery. On August 14, 2024, at approximately 10:34 a.m. (i.e., the day after the Geeks Zone robbery), ARCHIE sold a cellular phone taken in the Geeks Zone robbery at an EcoATM located inside a Safeway Grocery store located at 6118 Arlington Boulevard, Falls Church, Virginia. Several minutes prior, the black male using the same District of Columbia driver's license bearing the name with initials K.M. attempted to sell a cellular phone stolen in the Geeks Zone robbery. An image from the EcoATM showed ARCHIE standing next to the black male.

44. On August 29, 2024, ARCHIE was arrested for possession of stolen property by FCPD. During a recorded interview, ARCHIE admitted to being the driver during the Geeks Zone robbery, to selling the phones at the EcoATMs, and to being aware that "Cosmo" (who law enforcement has identified as PAIGE) and KIRKLAND had guns; ARCHIE claimed she felt threatened and was forced to participate.

45. During the course of the investigation, law enforcement identified the black male shown with ARCHIE at the EcoATMs as KIRKLAND. KIRKLAND was on GPS monitoring as a condition of his pretrial release for a pending D.C. Superior Court case. Preliminary GPS records received by law enforcement showed KIRKLAND's GPS placed him in the area at the dates and times of the Boost Mobile and Geeks Zone robberies. (Official GPS records obtained from the District of Columbia Pretrial Services after KIRKLAND's arrest showed that KIRKLAND was in and around the area at the times of both robberies; at the Exxon when PAIGE was there on July 25, 2024; at the Red Roof Inn consistent with the times the Honda was there on August 13, 2024; and at the Walmart after the Geeks Zone robbery.)

46. On August 29, 2024, KIRKLAND was arrested at his residence in Falls Church, Virginia by FCPD during the execution of a search warrant. During the search of the residence, FCPD seized items including a handgun with a tan/brown slide that was found in a bag also containing a credit card in KIRKLAND's name; that handgun was consistent in shape and size with the handgun carried by Subject 1 in the Geeks Zone robbery. Also found in the residence was another handgun, as well as a cellular phone and iPad box with IMEI numbers associated with stolen merchandise from the Geeks Zone.

47. Cellular phone records were obtained and revealed that ARCHIE's phone number was in contact with KIRKLAND's phone number, including before, the day of, and after the Geeks Zone robbery.

48. Records were also obtained from the Virginia Department of Corrections. Those records showed that PAIGE and KIRKLAND were incarcerated at the same correctional institution in 2023. Pictures of PAIGE also showed the distinctive tattoo of a woman's face on his arm, as also seen in the Exxon video.

PROBABLE CAUSE AS TO THE KIRKLAND DEVICES

49. During the August 29, 2024 search of KIRKLAND's residence, law enforcement seized the fourteen cellular telephones described herein as the **KIRKLAND DEVICES**. The aforementioned bag containing a credit card in KIRKLAND's name and a handgun consistent with that carried in the Geeks Zone robbery also contained nine cellular phones, all of which were seized by law enforcement. Five of the cellular phones found in that bag had IMEI numbers visible

and four did not.⁴ Of the phones with IMEI numbers visible, two of those phones were connected to the Geeks Zone robbery based on their IMEI numbers and the other three had IMEI numbers that were not on the stolen inventory list for either Boost Mobile or Geeks Zone.

50. KIRKLAND's residence was a one-bedroom apartment that he shared with his mother. KIRKLAND was believed to be sleeping in a makeshift bedroom just off the kitchen. In this area, law enforcement found an additional credit card and Medicaid card—both in KIRKLAND'S name. In addition to the nine cellular phones seized from the bag, law enforcement seized an additional five phones from the general area of the makeshift bedroom. None of the five other phones had IMEI numbers visible.

51. Based on my training and experience, there is probable cause to believe that the **KIRKLAND DEVICES** contain evidence, fruits, instrumentalities, and/or contraband of the Boost Mobile and Geeks Zone robberies for the following reasons, together with the reasons stated elsewhere in this Affidavit, among others:

- a. Through cooperation with EcoATM numerous stolen phones have been returned to law enforcement, which had been sold to their kiosks. Not only will this search warrant aid in discovering additional evidence specifically discussed below, but it will allow investigators to further identify stolen property.

⁴ “This number is a 15-digit identification number unique to your device. The IMEI number is different from a serial number and is used to identify and track devices for a number of purposes. Devices that come equipped with IMEI numbers include smartphones, tablets, and other mobile devices. These codes are used by carriers to identify a device on a mobile network, and they are often used by both carriers and law enforcement to block stolen or lost devices from accessing a network.” See <https://www.t-mobile.com/dialed-in/wireless/what-is-an-imei-number>.

- b. It is common for individuals engaged in the TARGET OFFENSES to use telephonic communications to further their criminal activities, by coordinating the concealment and disposal of stolen cash, clothing, firearms, and other instrumentalities of the crimes.
- c. Individuals engaging in the TARGET OFFENSES often use telephonic communications and other technology associated with cell phones to communicate and remain in contact with associates and potential associates, to plan future offenses, coordinate the sale of proceeds from such offenses, and coordinate other criminal activity. Because of the need to launder and conceal the proceeds of crimes like the TARGET OFFENSES, individuals' electronic devices may contain evidence of the TARGET OFFENSES weeks or months after the TARGET OFFENSES have been completed. This is particularly true if the proceeds obtained from the TARGET OFFENSES were large in amount or quantity.
- d. Individuals who engage in the TARGET OFFENSES often use cellular telephones to exchange information with potential associates through text messaging and instant messaging in addition to direct telephone conversations.
- e. It is also common for such individuals to send photographs and videos as exchanges of information with associates and/or potential associates.
- f. Cellular telephones used by individuals who engage in the TARGET OFFENSES contain valuable information and evidence relating to their activities. Such information consists of, but is not limited to: call logs, phone books, photographs, voice mail messages, text messages, images and video, Global Positioning System data, and any other stored electronic data. This information can: (i) reflect the

preparation for, arrangement of, and commission of the TARGET OFFENSES; (ii) reflect the ownership and use of the cellular telephones, firearms, cash, and other items by the individuals; (iii) document meetings and communications between these individuals, their associates, and/or their co-conspirators; (iv) reflect communications between these individuals and others discussing the TARGET OFFENSES; (v) reflect communications with others who may have assisted or provided support in these activities; (vi) document or contain evidence of the obtaining, secreting, transfer, expenditure and/or the concealment of contraband; and (vii) document or contain evidence of the purchase of items from the assets derived from the trafficking, theft, transportation, possession, or sale of contraband.

- g. Individuals involved in the TARGET OFFENSES often use cellphone cameras to take video recordings and photographs of themselves or other members of the conspiracy, sometimes, engaging in illegal activities, such as the brandishing or display of firearms or of items that have been stolen.
- h. Because individuals often carry their cell phones with them on their person while in transit, the phone user's movements can be tracked by examining the location of their cell phone over time. Analyzing the user's location information can therefore assist law enforcement in determining the user's location prior to and during each of the robberies and subsequent transactions at the EcoATMs.
- i. Individuals who commit crimes like the TARGET OFFENSES, frequently use multiple electronic devices in order to avoid detection by law enforcement. Furthermore, it is common for criminal actors to utilize false or incomplete addresses while filling out subscriber information related to their cellular telephones.

TECHNICAL TERMS

52. Based on my training, experience, and research, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of a network of NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- d. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those

functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
 - f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
 - g. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
53. Based on my training, experience, and research, I know that the **KIRKLAND DEVICES** all have capabilities that allow them to function as wireless telephones.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

54. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

55. There is probable cause to believe that things that were once stored on the **KIRKLAND DEVICES** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, devices’ internal hard drives—contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

56. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **KIRKLAND DEVICES** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **KIRKLAND DEVICES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other

external storage media, and the times the device was in use. Device file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

- f. I know that when an individual uses a device to coordinate crimes such as the TARGET OFFENSES, the individual's device may serve as a storage medium for evidence of the crime. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.
2. *Necessity of seizing or copying entire devices or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
 - a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly

examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

57. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **KIRKLAND DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether those parts are evidence described by the warrant.

58. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

59. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **KIRKLAND DEVICES**, further described in Attachment A, to seek the items described in Attachment B. Accordingly, I respectfully request that the Court issue the proposed search and seizure warrant.

Respectfully submitted and attested to in accordance with the requirements of Fed. R. Crim. P. 4.1 via telephone on January 13, 2025:

**CHARLES
ROONEY** Digitally signed by
CHARLES ROONEY
Date: 2025.01.13
14:09:53 -05'00'

Charles Rooney
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me by telephone in accordance with Fed. R. Crim. P. 4.1 on January 13, 2025:

 Digitally signed by Ivan Davis
Date: 2025.01.13 15:34:34 -05'00'

The Honorable Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

The property to be searched includes fourteen cellular telephones, currently in the custody of the FBI at the FBI's Northern Virginia Resident Agency, 9325 Discovery Boulevard, Manassas, VA 20109, within the Eastern District of Virginia. These devices, described in greater detail below, are associated with a person named VINCENT HENRY KIRKLAND, JR.

Search Warrant Number	Device Description
1:25-sw-17	Black iPhone, crack on front left corner and several cracks on back (FCPD Item #9)
1:25-sw-18	Black Samsung, with case, QR sticker on back, glossy finish back (FCPD Item #10)
1:25-sw-19	White iPhone S, Model A1633, FCC ID: BCG-E2946A, IC: 579C-E2946A (FCPD Item #11)
1:25-sw-20	Black iPhone, purplish face, Apple logo on back (FCPD Item #12)
1:25-sw-21	Black iPhone, Model A1778, FCC ID: BCG-E3091A, with retail sticker/barcode on back (FCPD Item #13A)
1:25-sw-22	Gray Motorola, with Motorola symbol on back, 50MP/Quad Pixel (FCPD Item #13B)
1:25-sw-23	Black Samsung, IMEI 350239335722617, QR sticker on back (FCPD Item #13C)
1:25-sw-24	Gray Motorola Razr (FCPD Item #13D)
1:25-sw-25	Black Samsung, IMEI 359147523653240 (FCPD Item #13E)
1:25-sw-26	Gray Motorola, with Motorola symbol on back, 50MP/Quad Pixel (FCPD Item #13F)
1:25-sw-27	Blue Samsung, IMEI 352271522724674, QR sticker on back (FCPD Item #13G)
1:25-sw-28	Silver iPhone, Model A1522, FCC ID: BCG-E2817A, IC: 579C-E2817A, IMEI: 354451060223564 (FCPD Item #13H)
1:25-sw-29	Purple iPhone, QR sticker on back with numbers 30202408131 40940369906 (FCPD Item #13I)
1:25-sw-30	Blue iPhone, with clear Pure Gear case, Apple sticker on back (FCPD Item #14)

This warrant authorizes the forensic examination of the cellular telephones for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to Be Seized

Evidence, fruits, instrumentalities, and/or contraband of 18 U.S.C. § 924(c)(1)(A)(ii) (use of a firearm during and in relation to a crime of violence), 18 U.S.C. § 1951 (obstruction of interstate commerce by means of robbery), 18 U.S.C. § 922(g) (possession of a firearm by a prohibited person), and 18 U.S.C. § 371 (conspiracy), as they relate to the robberies of the Boost Mobile Store located at 6531 Little River Turnpike, Alexandria, Virginia, and the Geeks Zone located at 15060 Cardinal Drive, Woodbridge, Virginia that took place in July and August of 2024, respectively (the “TARGET OFFENSES”), including but not limited to the following:

- a. Communications, records, information, photographs, videos, data, and/or other items reflecting the planning of, execution of, discussion of, proceeds from, and/or concealment of the TARGET OFFENSES;
- b. Communications about the TARGET OFFENSES among or about VINCENT HENRY KIRKLAND, JR., JAVON RUSTIN LOUIS PAIGE, and BRIANNA MAMIE OCEOLIA ARCHIE, and/or records, information, photographs, videos, data, and/or other items that tend to show the association or relationship among KIRKLAND, PAIGE, and ARCHIE and/or any other coconspirators in the TARGET OFFENSES;
- c. Communications, records, information, photographs, videos, data, and/or other items that tend to reveal the identities and/or the prior relevant whereabouts of KIRKLAND, PAIGE, and ARCHIE and/or any other coconspirators in the TARGET OFFENSES;
- d. Communications, records, information, photographs, videos, data, and/or other items relating to Boost Mobile and Geeks Zone, including the shopping centers surrounding them, the other surrounding areas, routes to and from the stores, knowledge of the stores’ employees or personnel or customers, and/or prior purchases or visits to the stores;
- e. Communications, records, information, photographs, videos, data, and/or other items discussing the acquisition, possession, and/or use of firearms;

- f. Communications, records, information, photographs, videos, data, and/or other items relating to clothing worn, items used, and/or vehicles used during and/or in advance of the TARGET OFFENSES;
- g. Communications, records, information, photographs, videos, data, and/or other items confirming the identities of the individuals using and/or owning telephone numbers, social media accounts, email addresses, addresses, vehicles, and electronic accounts relevant to the TARGET OFFENSES;
- h. Communications, records, information, photographs, videos, data, and/or other items relating to the cash, merchandise, and personal items stolen in connection with the TARGET OFFENSES and/or any other proceeds of the TARGET OFFENSES, including the possible concealment or laundering of those proceeds;
- i. Records reflecting the ownership and use of electronic devices that contain records of the commission of the TARGET OFFENSES;
- j. Contextual information necessary to understand the evidence described in this Attachment, including records and information that identify the creator or recipient of, or establish the time of creation or receipt of, the evidence described herein;
- k. Address/phone books and contact lists relevant to the TARGET OFFENSES;
- l. GPS, digital map, and/or location information relevant to the TARGET OFFENSES;
- m. Evidence indicating how and when accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the TARGET OFFENSES;
- n. Evidence of user attribution, showing who used or owned relevant devices at the time the things described in this warrant were created, edited, or deleted (such as logs, phonebooks, saved usernames and passwords, documents, account subscriber information, geographic location information, and browsing history); and
- o. Records evidencing the use of Internet Protocol addresses, including: (i) Records of Internet Protocol addresses used; and (ii) records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. Such records, communications, and information include text messages, instant messages, voice mail messages, photographs, images, videos, e-mails, notes, reminders, calendar entries, documents, internet history, bookmarked and favorite web pages, cookies, deleted files, call logs, location data, financial account information and records, and the content from messaging applications.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may

resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.